REMARKS

Claim Amendments

Claims 1, 6, 9, 13-15, 19 and 21 have been amended and claims 22-39 have been added. Claims 3-5, 7-8, 10-12, 16-18, and 20 have not been amended. Upon entry of this amendment, claims 1 and 3-39 will be in the application.

Independent claims 1, 6, 13, and 19 have been amended to clarify that the combination of user authorization and use of any of the several different data keys allows for retrieval and decoding "of the same security data" as opposed to different security data for different application programs. Claim 9 has been amended to correct antecedent basis. Claims 14, 15, and 21 have been amended to modify the language in the preamble. New claims 22-39 are "computer system" claims that substantially correspond to method claims 1 and 3-21. No new matter has been entered by these amendments.

Section 102(e) and 103(a) Rejections

Claims 1 and 3-5 (claim 2 has been canceled) stand finally rejected under 35 U.S.C. §102(e) as allegedly being anticipated by Lockhart et al. (US 6,230,272). Claims 6-10, 13-15 and 18-21 stand finally rejected under 35 U.S.C. §102(e) as allegedly being anticipated by Bjorn (US 6,035,398). Also, claims 11, 12, 16, and 17 stand finally rejected under 35 U.S.C. §103(a) as allegedly being obvious over Bjorn in view of Gressel (US 6,311,272). These rejections are respectfully traversed for the reasons given below.

The claimed method of securing security data, such as, *e.g.* a 128-bit encryption key, stored on a computer system, includes the steps of providing one of several different data keys (*e.g.*, passwords) to the computer system and transforming the security data with one data key in a reversible fashion to produce "encoded secure data." The encoded secure data is stored such that a user authorization process (*e.g.*, fingerprint validation) may be used in combination with the one data key (password) to provide access to the encoded security data. In accordance with the claimed method, the same security data (*e.g.*, 128-bit encryption key) may be encoded with different data keys (*e.g.*, passwords) to enable different combinations of authorized users and data keys or passwords to permit retrieval and decoding of the same security data. The claimed methods of securing the same security data with biometric data

from several different persons and several different data keys to provide multiple login is not taught by the cited prior art.

In the "Response to Arguments" section of the Final Rejection (pages 2-3), the Examiner alleged that Lockhart et al. do indeed teach the limitation, originally presented in claim 2, of encoding a same security data with several different data keys to provide several different encoded data such that a combination of user authorization and any of the several keys allows for retrieval and decoding. In support of this allegation, the Examiner alleged that Lockhart et al. teach at column 3, lines 6-22, the use of a "multipurpose data string to encrypt private keys (security data) which needs a user PIN or password to access (user authorization)" and at column 5, lines 26-32 that a user can "use a different data string for another software application that is used on the computer." From this teaching, the Examiner concludes that "a different data string can be used to encode different keys for the different software applications present on the computer" and that such teachings suggest the claimed feature wherein "a same security data is encoded with said several different data keys to provide several different encoded secure data such at a combination of user authorization and any of said several different data keys allows for retrieval and decoding of the same security data." Applicant respectfully disagrees.

In contrast with the claimed features, Lockhart et al. teach that a different data string used to encrypt different private keys, for example, may be used for different software applications for both encrypting the data of the software applications and for authenticating the user. In other words, Lockhart et al. teach that different passwords may be used to access different software programs used on the same computer. The claimed method instead recites that the "same security data" (*e.g.*, the same encryption key) is encoded with several different data keys (or passwords) to provide several different encoded secure data associated with respective authorized users whereby different combinations of users and data keys may retrieve and decode the "same security data." Applicant submits that Lockhart et al.'s suggestion of using different data strings for different software applications falls far short of suggesting using different data strings (data keys) in combination with user authorization to retrieve and decode the "same security data." Put another way, Lockhart et al. do not teach using the same private keys for different software applications and do not teach encoding the same private keys using different data keys (data strings) for multiple logins of different

combinations of authenticated users of the same private keys. Inasmuch as this distinction is clearly supported by the claims and not taught by Lockhart et al., withdrawal of the rejection of claims 1 and 3-5 as being anticipated by Lockhart et al. is respectfully requested.

The Examiner has not addressed Applicant's arguments that neither Bjorn nor Gressel teach encoding the same security data with "several different data keys ... such that a combination of user authorization and any of said several different data keys allows for retrieval and decoding of the same security data." In fact, in the rejection of claims 6-10, 13-15, and 18-21 as allegedly anticipated by Bjorn, the Examiner cited to language from Lockhart et al. (top of page 6) without indicating where comparable teachings are provided by Bjorn. Applicant submits that, absent such teachings, Bjorn cannot anticipate the claimed invention. To rely upon such teachings, the Examiner would have to recast the rejection as an obviousness rejection and provide the requisite motivation to combine the teachings of Bjorn and Lockhart et al. In any case, Applicant submits that such a rejection would be improper because the requisite motivation to combine is not present and because neither Lockhart et al. nor Bjorn teaches the claimed multiple login technique for accessing the "same security data" as claimed. Withdrawal of the rejection of claims 6-10, 13-15 and 18-21 as allegedly being anticipated by Bjorn is thus believed to be proper and is respectfully solicited.

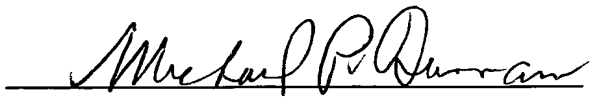
Given that Gressel does not provide teachings that address the above-mentioned shortcomings in Lockhart et al. and/or Bjorn, claims 11-12 and 16-17 are believed to be allowable for the same reasons as given above with respect to independent claims 6 and 13. Withdrawal of the rejection of claims 11-12 and 16-17 as allegedly being obvious over the teachings of Bjorn and Gressel is thus believed to be proper and is respectfully solicited.

Finally, new system claims 22-39 are believed to be allowable for substantially the same reasons as the corresponding method claims 1 and 3-21. Consideration and allowance of new claims 22-39 are respectfully solicited.

Conclusion

Amended independent claims 1, 6, 13, and 19 and new independent claims 22, 26, 33, and 38 are believed to be novel and nonobvious over the prior art cited by the Examiner. Withdrawal of all rejections and issuance of a Notice of Allowability are respectfully requested.

Date: June 23, 2006



Michael P. Dunnam
Registration No. 32,611

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439